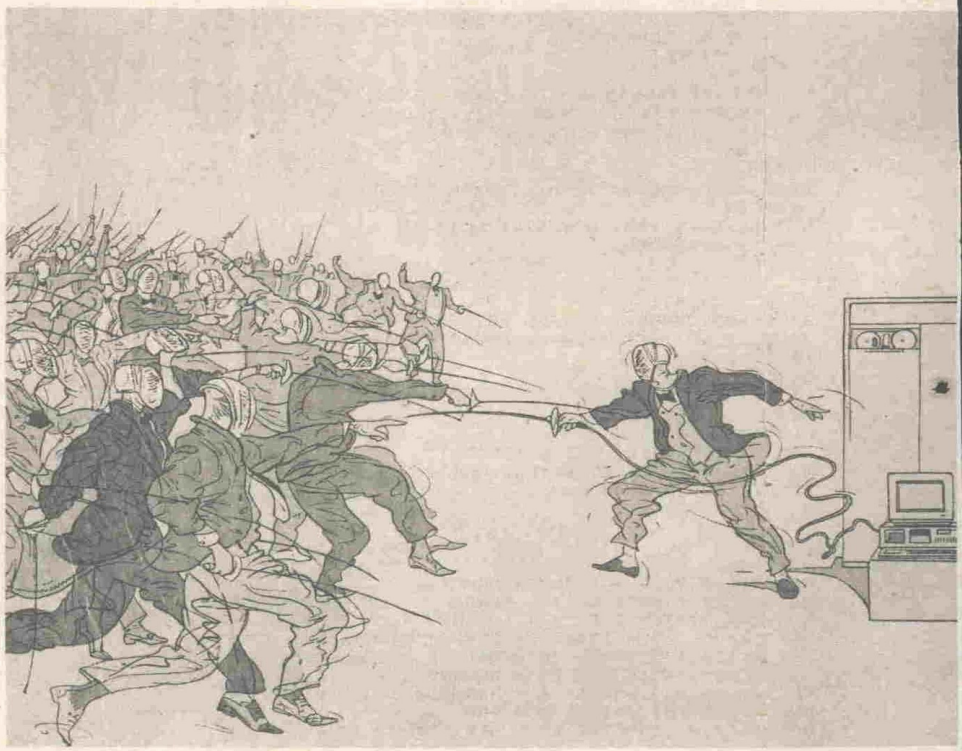
เอนก ศิรจริยาภิวัฒน์

หนทางต่อสู้และป้องกันไวรัส : หลากหลายกับ ไวรัสคอมพิวเตอร์

ลักษณะไวรัสชนิดต่าง ๆ หาหนทางแก้ไขอย่างไร วิธีหนึ่งควรแบคอัพไฟล์ และ Scan แผ่นแปลกปลอมที่เข้ามาในเครื่องเรา



คอมพิวเตอร์ไวรัส คำนี้อยู่กับคนไทยมาเป็นเวลานานนับปี จนกระทั่งปัจจุบันนี้ หลาย ๆ คนสรุปความผิดพลาดนั้นเกิดขึ้นมาจากไวรัสคอมพิวเตอร์ โดยเราเองไม่ได้นึกถึงสาเหตุอีกมากมายหลายประการที่ทำให้คอมพิวเตอร์สุดที่รักของเราทำงานผิดพลาด ลองดูปัญหาง่าย ๆ และมักพบบ่อย ๆ ดังรูปที่ 1 ว่าปัญหานี้เกิดจากไวรัสคอมพิวเตอร์หรือไม่? เราลองมาดูสาเหตุที่ทำให้คอมพิวเตอร์ทำงานไม่ได้หรือได้แต่ไม่ใช่ความต้องการของเราว่ามันมาจากสาเหตุใดบ้าง

การทำงานที่ผิดพลาดของผู้ใช้ (Operator error)

การทำงานบางอย่างที่ผิดพลาดเกิดจากความพลั้งเผลอหรือไม่เข้าใจคำสั่งเหล่านั้นอย่างลึกซึ้งเพียงพอ จึงทำให้เกิดสถานการณ์ที่น่าเศร้าใจอย่างยิ่ง ลองดูข้อผิดพลาดที่มักประสบกันบ่อย ๆ ดังนี้

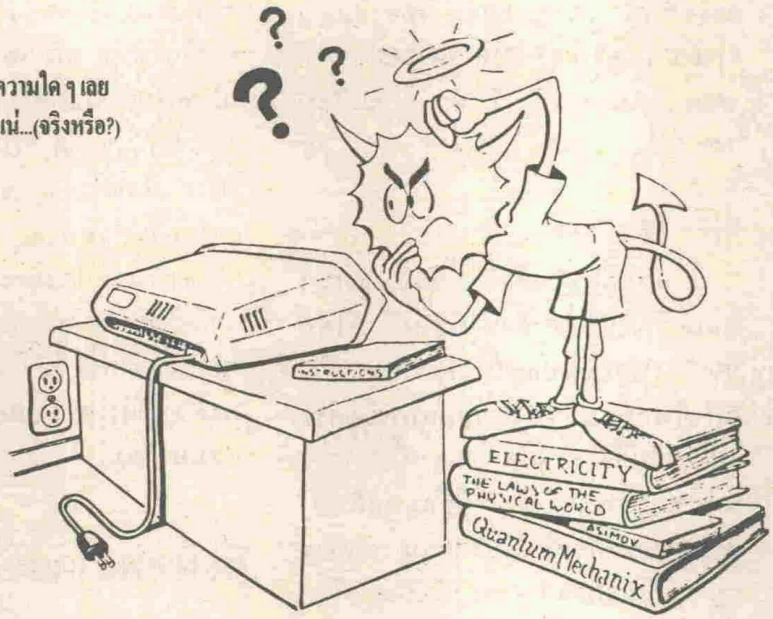
คำสั่ง DEL

คำสั่งนี้มักจะมีปัญหาเมื่อใช้คำสั่งว่า DEL *.* ลองมาดูเหตุการณ์สมมติที่เราจะสร้างขึ้นนี้ แล้วนึกถึงการทำงานไปทีละขั้น แล้วสรุปผลสุดท้ายว่าอะไรจะเกิดขึ้น ถ้าเราทำงานกับโปรแกรมโลตัส 123 โดยมีไดเรคทอรีที่ทำงานอยู่ 5 ไดเรคทอรี มีการตั้งชื่อไดเรคทอรีดังนี้ WORK1, WORK2, WORK3, WORK4 และ WORK5 โดยงานหลักเราใช้ไดเรคทอรี WORK1 เป็นสำคัญ เราทำงานมาเรื่อย ๆ วันหนึ่งเรานึกอยากจะเคลียร์งานในไดเรคทอรีต่าง ๆ ขั้นตอนแรกเมื่อเปิดเครื่องคอมพิวเตอร์ด้วยความเคยชิน เราก็จะเข้าไปที่ไดเรคทอรี WORK1 โดยใช้คำสั่ง

```
CD \123\WORK1
```

วันนี้เราอยากเคลียร์งานที่ไม่ทำแล้วทิ้งไป เราจึงเช็คงานต่าง ๆ โดยใช้คำสั่ง

```
DIR... \WORK2
```



รูปที่ 1
จอมืดไม่มีข้อความใด ๆ เลย
ต้องเป็นไวรัสแน่...(จริงหรือ?)

คอมพิวเตอร์จะแสดงรายชื่อไฟล์ข้อมูลในไดเรคทอรี WORK2 ให้ตกลงว่าเราดูแล้วว่างานนี้ยังไม่เสร็จสิ้นก็สั่งต่อ

DIR... \ WORK3

ปรากฏรายชื่อไฟล์ข้อมูลในไดเรคทอรี WORK3 ที่เราทำเสร็จสิ้นไปนานแล้วเราจึงอยากที่จะเคลียร์งานนี้ จึงใช้คำสั่ง

DEL *.*

พร้อมกับตอบคำถามของคอมพิวเตอร์ที่ถามเราว่า Are you sure? เราก็ตอบด้วยความแน่ใจว่า เราจะลบไฟล์ข้อมูลในไดเรคทอรี WORK3 นี้แหละ โดยตอบว่า Y กับคอมพิวเตอร์

เสร็จแล้วเราก็เช็คไดเรคทอรี WORK4 และ WORK5 ต่อไป เมื่อเสร็จสิ้นภารกิจทั้งหมด เราก็พร้อมที่จะทำงานในไดเรคทอรี WORK1 ต่อไป จึงเรียกโลตัสพร้อมใช้คำสั่ง FILE/RETRIVE ถึงตอนนี้ท่านผู้อ่านลองนึกเหตุการณ์เอาเองนะครับว่า เราจะใจหายหรือไม่ เมื่อเราพบว่าไม่มีไฟล์ข้อมูลของเราหลงเหลืออยู่เลย เพราะอะไรลองทบทวนเหตุการณ์ทั้งหมดดูนะครับ

เหตุการณ์ร้ายผ่านไปแล้ว วันต่อ ๆ มาเราคงได้บทเรียนว่า การใช้คำสั่ง DEL *.* เราต้องไปไดเรคทอรีที่เราต้องการลบเสียก่อน หรือไม่ก็ต้องระบุให้เต็มยศว่าจะลบไดเรคทอรีใด เช่น เหตุการณ์ที่ผ่านมาสิ่งที่ถูกคือใช้คำสั่ง DEL \ LOTUS \ WORK3 \ *.* แทนคำสั่ง DEL *.* บทเรียนนี้คงเป็นเรื่องเตือนใจที่ดี แต่วันต่อมาเราต้องเคลียร์งานอีกแล้ว (ได้ยินคำนี้ซักผวา) โดยเราได้รับเงินค่าตอบแทนจากบริษัทอาภาภรณ์ (บริษัทสมมติ) เราจึงอยากเคลียร์งานของบริษัทนี้ โดยเรารู้เองว่าบริษัทนี้ทำกิจการเกี่ยวกับเสื้อผ้า ซึ่งเราใช้ไดเรคทอรี WORK4 ไว้สำหรับเก็บข้อมูลของบริษัทขายเสื้อผ้า และเราก็ใช้ 3 ตัวอักษรหลังของชื่อไฟล์ข้อมูลเป็นรหัสแทนชื่อบริษัท และเราก็ตรวจสอบแล้วว่าบริษัทอาภาภรณ์มีรหัส 003 เราก็เลยจะลบไฟล์ข้อมูลของบริษัทนี้เสียโดยทำตามขั้นตอนดังนี้

CD \ LOTUS \ WORK4

คราวนี้ไม่ผิดแน่เมื่อเข้าไดเรคทอรีที่เราจะกระทำอะไรกับไฟล์ข้อมูลที่เราต้องการ เมื่อเข้ามาถูกไดเรคทอรี เราจึงใช้คำสั่งดังนี้

DEL *003.*

โดยเราเข้าใจว่า คำสั่งนี้คือลบไฟล์ข้อมูลที่ชื่อขึ้นต้นด้วยอะไรก็ได้ แต่ลงท้ายด้วย 003 เครื่องคอมพิวเตอร์ก็จะถามเราว่า Are you sure? เราก็นึกว่าเราลบหลายไฟล์พร้อมกัน เครื่องคอมพิวเตอร์จึงถามเพื่อความแน่ใจ เราจึงตอบ Y ลงไป เสร็จสิ้นทั้งหมดแล้ว เราก็ถอนหายใจพร้อมกับยิ้มที่มุมปากเล็กน้อย เพราะงานของบริษัทอาภาภรณ์เสร็จแล้วและก็รับเงินมาแล้วด้วย วันนี้ก็โชคดีที่บริษัทที่จะมาทำงานต่อไปก็เป็นบริษัทขายเสื้อผ้าเหมือนกัน จึงไม่ต้องเปลี่ยนไดเรคทอรีเลย เราจึงเรียกโลตัส 123 พร้อมคำสั่ง FILE/RETRIVE อะไรจะเกิดขึ้นหรือนี่ ไฟล์ข้อมูลหายไปไหนหมด ใครมาแกล้งเรานะ แก้นจริง ๆ

คำเฉลยปริศนานี้ก็คือไม่ได้มีใครแกล้งเราหรอก แต่เป็นเพราะว่าคำสั่ง DEL *003.* นั้นเครื่องคอมพิวเตอร์ (DOS) เข้าใจว่าเราต้องการลบไฟล์ข้อมูลทั้งหมดเลย คำสั่งลบข้อมูลที่ขึ้นต้นด้วย * และมีนามสกุลเป็น * ก็จะหมายถึงไฟล์ทั้งหมดนั้นเอง พอถึงตอนนี้ ถ้าใครเจอเหตุการณ์นี้จริงคงผวากับคำว่าเคลียร์งานเป็นแน่แท้ (เป็นโรคคอมพิวเตอร์ชนิดใหม่คือกลัวคำว่าเคลียร์งาน)

คำสั่ง SYS

คำสั่งนี้ใช้สำหรับคัดลอก system file ไปยังไดร์ฟที่เราต้องการ ในคู่มือของดอสจะระบุว่าเราสามารถเปลี่ยนดอสของฮาร์ดดิสค์โดยใช้คำสั่งเพียง

SYS C: แต่ก็มีผู้ประสบเหตุมาแล้วว่าคำสั่งนี้ทำงานได้ประมาณ 99.9% โดยเหตุการณ์นั้นเกิดจากที่ดอสแต่ละรุ่นและแต่ละบริษัท บางทีก็มีความแตกต่างกันบ้าง ดอสตัวใหม่อาจไม่เข้าใจโครงสร้างของฮาร์ดดิสค์ (layout of disk) ของดอสตัวเก่า (ดอสเวอร์ชัน 4.X และ compaq dos 3.31 จะสามารถฟอร์แมตฮาร์ดดิสค์ได้เกินพาร์ติชั่นละ 32 เมกะไบต์ ซึ่งทำให้โครงสร้างของดิสค์ผิดกันไปจากดอสตัวเก่า ๆ) ถ้าดอสตัวใหม่สามารถอ่านเขียนดิสค์ได้แต่ไม่เข้าใจโครงสร้างดิสค์ของดอสตัวเก่าว่า FAT และไดเรคทอรีเป็นอย่างไร ก็จะทำให้ข้อมูลของอาจหายสาบสูญไปเลยก็ได้ (sending your data off into Limbo ในความเห็นส่วนตัวผมชอบประโยคนี้มาก แต่ก็ไม่อยากเจอสักเท่าไร) เพราะฉะนั้น จึงเป็นข้อเตือนใจว่าจะทำอะไรกับฮาร์ดดิสค์ควรแบคอัพข้อมูลเสียก่อน แบคอัพข้อมูลซะเถอะนะครับ เขียนคำขวัญไว้ข้างโต๊ะของเราเองเลยว่า "แบคอัพข้อมูลเสียก่อนก่อนที่จะไม่มีข้อมูลให้แบคอัพ" หรือไม่ก็ให้โหด ๆ หน่อย โดยขู่ไว้ว่า "แบคอัพข้อมูลซะ มิฉะนั้นเราจะ sending your data off into Limbo" อีกเหตุการณ์หนึ่งก็คือมีผู้พบว่า ถ้าเราใช้ฮาร์ดดิสค์ขนาด 40 เมกะไบต์ และมีขนาดเซกเตอร์ 1 กิโลไบต์ เราไม่ควรบูตเครื่องจากดอสอื่น ๆ ที่ไม่ใช่ตัวที่บรรจุอยู่ในฮาร์ดดิสค์ ถ้าบูตไปแล้วและต้องการใช้ต่อ ควรใช้คำสั่ง DIR เช็คว่าดอสตัวนั้นเข้าใจระบบไฟล์ของฮาร์ดดิสค์เราหรือเปล่า ก่อนที่จะเขียนข้อมูลอะไรลงไปที่ฮาร์ดดิสค์ เพราะมีเหตุการณ์น่าเศร้าเกิดขึ้นก็คือ ดอสตัวที่เปิดเครื่อง (strange DOS) ทำลายระบบไฟล์ของฮาร์ดดิสค์ (scrembling the filing system) โดยผู้เล่า (DR. SOLOMON) บอกว่าพบเหตุการณ์นี้ประมาณเดือนละครั้ง

คำสั่ง RECOVER

ด้วยชื่อของคำสั่งนี้จึงมีหลาย ๆ คนเข้าใจว่าเป็นคำสั่งที่ใช้สำหรับกู้ไฟล์ข้อมูล (UnDeleting Utility) เหตุการณ์ก็คือไฟล์ข้อมูลของเราถูกลบหรือหายไปโดยไม่ตั้งใจ เมื่อเป็นเช่นนี้หลาย ๆ คนก็พยายามหาวิธีการกู้ข้อมูลกลับมา เมื่อเจอแผ่นดอสที่มีโปรแกรม recover อยู่ ก็นึกไปเองว่าคงจะใช้กู้ข้อมูลโดยสั่งว่า

```
recover a:
```

ผลที่ตามมาก็คือไฟล์ใน drive ไม่มีอะไรเหลืออยู่เลยนอกจากไฟล์ชื่อ FILE0000.REC, FILE0001.REC และ FILE0002.REC ต่อกันไปเรื่อย ๆ ซึ่งเป็นผลที่น่าเศร้าใจอย่างยิ่ง จึงเป็นข้อเตือนใจว่าคำสั่งนี้จะใช้เมื่อยามคับขันเท่านั้น ใช้ในการกู้แผ่นดิสค์ที่มี Bad sector และไม่สามารถทำอะไรกับดิสค์นั้นได้แล้ว หรือมีไฟล์บางไฟล์ที่มี Bad sector อยู่ (รายละเอียดมากกว่านี้ควรดูจากคู่มือดอสให้ละเอียดถ่องแท้ เช่น การ recover เป็นไฟล์) คงต้องจำไว้ให้มั่นว่าโปรแกรม Recover ไม่ใช่โปรแกรมที่ใช้สำหรับกู้ข้อมูลไฟล์ที่ถูกลบไป (UnDeleting Utility) ซึ่งเรื่องนี้คู่มือดอสน่าจะบอกไว้ด้วย

โปรแกรมยูทิลิตี้

โปรแกรมจำพวกนี้มีขายกันอยู่มากมายเกลื่อนตลาด ยิ่งเกิดสภาวะไวรัสขึ้น หลาย ๆ คนก็พยายามที่ลองเล่นลองใช้โปรแกรมยูทิลิตี้ด้วยความหวังดีกับหน่วยงานของตน แต่บางครั้งผลที่ตามมาร้ายแรงยิ่งกว่าการทำลายของไวรัสหลายสิบเท่าตัว สาเหตุเพราะโปรแกรมเหล่านี้มีการยอมรับให้แก้ข้อมูลส่วนสำคัญของดิสค์ได้เช่น ตารางพาร์ติชั่น โดยการแก้ไขไม่ได้มีการยืนยันการแก้ไขส่วนสำคัญ ๆ เหล่านี้เลย เช่น ถามว่า Are you sure? เหมือนที่ดอสทำ ผลที่เกิดขึ้นบางครั้งจึงเกินความคาดคิดได้ (บางครั้งก็ยังโชคดีที่มีโปรแกรม NDD ของนอร์ตันยูทิลิตี้ที่สามารถกู้กลับมาได้)

ข้อผิดพลาดของโปรแกรม (Bugs)

เรื่องข้อผิดพลาดของโปรแกรมเป็นเรื่องใหญ่และบางครั้งเราเองต้องยอมรับสถานการณ์เหล่านั้น สาเหตุสำคัญก็มาจากที่โปรแกรมมีขนาดใหญ่และซับซ้อนมากขึ้นเรื่อย ๆ นั่นเอง การพัฒนาโปรแกรมขนาดใหญ่นั้น จำเป็นต้องใช้โปรแกรมเมอร์จำนวนมากมาย เช่น โลตัส ต้องใช้โปรแกรมเมอร์ประมาณ 200 คน ถ้าเกิดโปรแกรมเมอร์คนใดคนหนึ่งทำโปรแกรมพลาด ซึ่งแน่นอนว่ามีผลกระทบกับโปรแกรมสำเร็จรูปที่ผลิตออกมานั้นเอง เรื่องนี้มีวิธีทดสอบก็คือส่งให้ลูกค้าประจำหรือทดสอบกันเอง ซึ่งถ้าจะทดสอบจนแน่ใจ 100% ว่าโปรแกรมไม่มีข้อผิดพลาดนั้นต้องใช้เวลาเป็นแรมปีแน่ จึงไม่แปลกที่เราจะเจอกับโปรแกรมที่มีข้อผิดพลาด แม้กระทั่งดอสเองก็มีปัญหา (ซึ่งน่าจะแก้ไขมานานแล้วแต่ก็ยังไม่ได้แก้ไขสักที) เราลองมาดูปัญหาของดอสว่าเกิดอะไรขึ้น (ทั้ง ๆ ที่ไม่น่าจะเกิดขึ้น) สิ่งที่ต้องเตรียมก็คือดิสค์ 2 แผ่น แผ่นแรกติด write protect มีไฟล์อยู่จำนวนหนึ่ง แผ่นที่ 2 เป็นแผ่นที่ไม่

ติด write protect และเป็นแผ่นว่างหรือแผ่นที่มีข้อมูลซึ่งเราไม่ต้องการใช้แล้ว

- ใส่แผ่นแรกไว้ที่ไดรฟ์ A:
- เขียนข้อความอะไรก็ได้ไปที่ไดรฟ์ A: โดยใช้คำสั่ง

```
copy con a : test.dat
```

เสร็จแล้วพิมพ์ข้อความอะไรก็ได้ จบด้วยการกด F6 และรีเทอร์น

- ตอนนี้ดอสจะพยายามเขียนข้อมูลลงแผ่นแรกซึ่งติด write protect อยู่ จึงเขียนไม่ได้ทำให้มีข้อความว่า

```
write protect error writing drive A
Abort, Retry, Fail?
```

หมายเหตุ คำว่า Fail อาจเป็นคำว่า ignore แทน

- เอาแผ่นแรกออกเสร็จแล้วเอาแผ่นที่สอง (ไม่ติด write protect) ใส่แทน แล้วกด R ซึ่งหมายถึง Retry
- ตรวจผลการทำงานดูโดยใช้คำสั่ง

```
DIR A:
```

ผลที่ได้คือชื่อไฟล์บนแผ่นที่สองถูกแทนที่ด้วยชื่อไฟล์ของแผ่นแรก

เห็นผลงานของดอสแล้ว เราคงได้ข้อคิดแล้วว่าถ้าแผ่นที่สองเป็นแผ่นที่เราใช้งานอยู่ เราคงจะไม่เหลืออะไรอยู่เลย ข้อควรจำก็คือถ้าเราไม่แน่ใจในผลงานของดอสแล้วเราควรเลือก A-Abort เสียดีกว่า ทำใหม่อีกครั้งดีกว่าของเก่าไม่มีเหลืออยู่

ปัญหาของตัวเครื่อง(Clashes)

เครื่องในเมืองไทยตอนนี้ทุกคนคงยอมรับว่ามาจากได้หวันเสียส่วนมาก ซึ่งเป็นของประเภท noname (หรือทำให้มี name โดยเอาชื่ออะไรก็ไม่รู้มาติด) เมื่อเราพร้อมใจเต็มใจที่จะใช้ของ no-name เราก็ต้องเตรียมใจกับปัญหาต่าง ๆ ที่จะเกิดขึ้น เช่น เครื่องหยุดทำงานลงเฉย ๆ โดยไม่ทราบสาเหตุ แต่กระนั้นไม่ใช่ว่าใช้ของมีชื่อจะไม่มีปัญหาใด ปัญหานั้นเกิดกับเครื่องได้เสมอ ๆ เมื่อก่อนนี้เครื่องคอมพิวเตอร์แทบจะเหมือนพระเจ้าต้องอยู่ในห้องแอร์และปราศจากฝุ่น แต่ปัจจุบันบางท่านก็ลืมนึกถึงสิ่งเหล่านี้เสียแล้ว สิ่งที่น่ากลัวและกำลังเป็นปัญหาตอนนี้ก็คือ ผู้ผลิตไอซีชิพเร่งทำงานเพื่อให้ทันตลาดจนบางครั้งเกิดปัญหา (Bug) กับชิพเหล่านั้น ซึ่งบางครั้งบริษัทผู้ผลิตเครื่องคอมพิวเตอร์หรือนักวิจัยได้ผลิตเครื่องออกขายออกสู่ท้องตลาดแล้ว แม้กระทั่ง 80486 เราก็คงได้ยินข่าวว่าเกิดปัญหาขึ้นเรื่องนี้บางครั้งจึงโทษบริษัทผู้ผลิตเครื่องคอมพิวเตอร์หรือนักวิจัยไม่ได้ จึงต้องทำใจกับสถานการณ์เร่งรีบกันแข่งขันในตลาดขณะนี้ แต่ก็อย่าได้ถึงกับตกใจกับเหตุการณ์เหล่านี้ เพราะจริง ๆ แล้วการเกิดข้อผิดพลาดของชิพยังเป็นจำนวนน้อยมากเมื่อเทียบกับชิพที่อยู่ในท้องตลาดขณะนี้

โทรจัน (Trojans)

คำนี้หลาย ๆ คนลืมนึกถึงไปแล้ว โดยเรียกเป็นไวรัสแทน ความหมายของโทรจันก็คือโปรแกรมที่หลอกให้ผู้ใช้ใช้งาน แต่มีบางส่วนทำลายข้อมูลบนดิสก์เรา ตัวที่กำลังฮือฮากันตอนนี้ก็คือ AIDS โดยโปรแกรมบอกว่าตัวมันเองเป็นแหล่งข้อมูลที่ให้ความรู้เกี่ยวกับโรค AIDS แต่ตัวมันเองก็ทำลายข้อมูลบนดิสก์ทิ้ง

ไวรัส (Viruses)

คำนี้คงไม่ต้องนิยามกันใหม่เพราะคงได้ยินกันจนชินหูแล้ว สิ่งที่จะนำมาให้ท่านผู้อ่านอ่านก็คือรายชื่อและอาการของไวรัสต่าง ๆ ซึ่งข้อมูลนี้ได้มาจากวารสาร VIRUS BULLETIN ซึ่งไม่ใช่ข้อมูลที่ใหม่นัก (เดือนธันวาคม 2532) แต่ยังไม่เห็นผู้เผยแพร่ จึงนำมาให้อ่านกัน โดยข้อมูลจะเริ่มจากชื่อตามด้วยวงเล็บระบุชนิดซึ่งมีรายละเอียดดังนี้

C หมายถึง โจมตีกับไฟล์นามสกุล .COM

E หมายถึง โจมตีกับไฟล์นามสกุล .EXE

D หมายถึง โจมตีกับ DOS boot sector (Logical sector 0) บนฮาร์ดดิสก์และฟลอปปี้ดิสก์

M หมายถึง โจมตีกับ Master boot sector (Absolute sector 0 บนฮาร์ดดิสก์และฟลอปปี้ดิสก์)

N หมายถึง ไม่ฝังตัวเองบนหน่วยความจำ

R หมายถึง ฝังตัวเองบนหน่วยความจำ (resident in memory)

ข้อมูลที่ได้จากวารสารนี้ เป็นข้อมูลที่น่าสนใจมาก โดยมีตัวอย่างรายละเอียดไวรัสสำหรับประจำเดือนธันวาคม 2533 ดังรูปที่ 2 ถ้าใครสนใจวารสารนี้ สามารถติดต่อได้ที่

VIRUS Bulletin Ltd, Haddenham, Aylesbury, HP 178JD England
Tel (0844), International Tel (+44) 844 290396
Fax (0844) 291409, International Fax (+44) 844 291409 หรือ
June Jordan, Virus Bulletin, PO Box 875, 454 Main Street, Ridgefield, CT06877
Tel 203 431 8720, Fax 203 431 8165

สมัครโดยจ่ายค่าสมาชิกใน 1 ปี

(12 ชุด) ในราคา $350 (first class airmail) ผมเองไม่ได้ค่าโฆษณาใด ๆ แต่อยากให้เมืองไทยมีแหล่งข่าวเกี่ยวกับไวรัสบ้าง ถ้าใครมีก็อย่าลืมเผยแพร่กันบ้างนะครับ อีกแหล่งที่จะหาข้อมูลและติดต่อเป็นอย่างยิ่ง (ทั่วโลกยอมรับ) คือผู้ผลิตโปรแกรม SCAN และ clean ซึ่งได้แก่

McAfee Associales
4423 Cheeney Street
Santa Clara, CA 95054
408 988 3832 Voice
408 970 9727 Fax

รูปที่ 2 รายละเอียดไวรัสสำหรับฉบับประจำเดือนธันวาคม 2532

405 [CN] ติดกับไฟล์ .COM โดยการเขียนข้อมูล 405 ไบต์กับข้อมูลเดิม ถ้าเกิดไฟล์เดิมเล็กกว่า 405 ไบต์ ขนาดไฟล์ใหม่ก็จะกลายเป็น 405 ไบต์แทนและจะแพร่เชื้อกับไดเรคทอรีปัจจุบัน (current directory) ตัวโปรแกรมไม่เช็คว่าไฟล์ .COM นั้นได้ติดเชื้อแล้ว

Alabama [ER] มีขนาด 1560 ไบต์ ยังไม่มีรายละเอียดเพิ่มเติม (Virus awaiting desassembly)

Brain, Ashar, shoe [DR] ติดเชื้อกับ bootstrap sector และเนื้อที่ดิสค์อีก 3 clusters (6 sector) โดยการเปลี่ยน FAT ที่ตำแหน่งนั้นเป็น Bad Cluster ติดกับดิสค์ประเภท 360 K เท่านั้น และกินหน่วยความจำไป 7 K เปลี่ยนลาเบลของดิสค์เป็น (C) Brain หรือบางครั้งก็เป็น (C) ashar

cascade, Fall, Russian [CR] ไวรัสตัวนี้จะติดกับ .COM ไฟล์ โดยมีการเข้ารหัส (encrypted) ตัวเอง การเข้ารหัสนี้จะขึ้นกับขนาดของไฟล์ เพราะฉะนั้นไฟล์ที่ขนาดต่างกันไวรัสตัวนี้จึงมีรูปร่างที่ต่างกัน ขนาดของไฟล์ที่ถูกแพร่เชื้อจะมีขนาดเพิ่มขึ้น 1701 หรือ 1704 ไบต์ ตัวต้นแบบ (original version) จะมีตัวอักษรหล่น (falling character) ในช่วงวันที่ 1 ตุลาคม ถึง 31 ธันวาคม ปี 1988 ส่วนตัวใหม่ (formatting version) จะทำการฟอร์แมตฮาร์ดดิสค์ในช่วง 1 ตุลาคมถึง 31 ธันวาคมของทุกปียกเว้นปี 1993 อาการจะปรากฏเมื่อไวรัสทำงานไปแล้วในช่วง 5 นาที

Cascade (1)-01 - Falling Characters
Cascade (1) 04 - Falling Characters
Cascade (1) Y4 - Falling Characters
Cascade format - Formats hard disk

Dark Avenger [CER] จะติดกับทุกไฟล์ที่ถูกเปิด (open), ปิด (close) หรือถูกปฏิบัติงาน (execute) โดยไฟล์นั้นต้องมีขนาดอย่างน้อย 1775 ไบต์ และจะเพิ่มขนาดของไฟล์ที่ติดเชื้อขึ้น 1800 ไบต์

Data crime [CN] ติดกับไฟล์ .COM เพิ่มขนาดขึ้น 1168 หรือ 1280 ไบต์ เมื่อไวรัสทำงานตัวไวรัสจะหาไฟล์ .COM ในทุกไดเรคทอรีของไดรฟ์ A,B,C และ D เมื่อไฟล์ใดยังไม่ติดเชื้อก็จะทำการแพร่เชื้อใส่ไฟล์ .COM นี้ ถ้าเกิดตัวอักษรตัวที่ 7 เป็นตัวอักษร D เช่น Command.com ก็จะไม่ถูกไวรัสชนิดนี้เล่นงาน ผลของไวรัสตัวนี้คือ หลังวันที่ 13 ตุลาคมของทุกปี จะทำการฟอร์แมตแทร็ก 0 ของฮาร์ดดิสค์ และจะฟอร์แมตฮาร์ดดิสค์แบบไม่เหลือข้อมูลอยู่ (low level format) หลังจากแสดงข้อความนี้ขึ้นมา

DATA CRIME VIRUS
RELEASED: 1 MARCH 1989

ข้อความนี้อยู่ในรูปการเข้ารหัสไว้ จึงไม่สามารถใช้โปรแกรมหาข้อความกับไวรัสตัวนี้ได้

Data crime II [CEN] ติดไฟล์นามสกุล .COM กับ .EXE เพิ่มขนาดขึ้น 1514 ไบต์ อาการเหมือน Data crime ตัวแรก แต่จะเปลี่ยนชื่อไฟล์ที่ไม่ติดเชื้อเป็นไฟล์ที่มีอักษรตัวที่ 2 เป็นตัว B และจะทำ low lever format หลังจากแสดงข้อความ

DATA CRIME II VIRUS

dBase [CR] สร้างไฟล์ชื่อ BUGS.DAT บน root directory ของไดรฟ์ C: อาการคือมีการสลับ (Transpose) ไฟล์ข้อมูลของ dBase (.DBF) จะทำให้เกิดความผิดพลาด (errors) เมื่อเดือนที่สร้างไฟล์ BUGS.DAT กับเดือนปัจจุบันห่างกัน 3 เดือน ไฟล์ที่ติดเชื้อเพิ่มขนาดขึ้น 1864 ไบต์

Den Zuk, Search [DR] ตัวไวรัสจะอยู่ที่แทร็ก 40, เฮด 0, เซกเตอร์ 33 ถึง 41 จะเกิดข้อความเลื่อน (sliding) ว่า DEN ZUK บนจอเมื่อกด Ctrl-Alt-Del

Fu Manchu [CER] ติดไฟล์ .COM (เพิ่มขนาด 2086 ไบต์) ยกเว้น command.com และไฟล์ .EXE (เพิ่มขนาด 2080 ไบต์) เป็นการเขียนขึ้นใหม่ของ Jerusalem Virus แต่จุดสังเกตจะเปลี่ยนเป็น rE-HMORr และคำว่า sU จะเปลี่ยนเป็น sAX โดยเป็นชื่อ →

รูปที่ 2 (ต่อ)

คนเขียนนั้นเอง (Sax Rohmer) ประมาณ 1 ใน 16 ของเวลาปกติ จะขึ้นข้อความว่า The world will hear from me again จะรีบูตระบบหลังจากทำงานไปแล้วด้วยเวลาที่หารด้วยครึ่งชั่วโมงได้ (ทุก ๆ ครึ่งชั่วโมงมีโอกาสเกิดเหตุการณ์ได้ ค่ามากสุดคือ 7.5 ชั่วโมง) ข้อความข้างต้นจะเกิดขึ้นอีกเมื่อมีการกด Ctrl-Alt-Del จะไม่มีการรีบูตระบบให้หลังจากวันที่ 1 สิงหาคม 1989 ไวรัสจะคอยเช็คข้อความที่พิมพ์ว่าเป็นชื่อนักการเมืองหรือไม่ (Thatcher, Reagan, Botha และ Waldheim) โดยจะใส่ข้อความเพิ่มเติมเข้าไปในทางที่ไม่ควร (derogatory comment) และแสดงข้อความว่า VIRUS 3/10/88 latest is the new fun line! เมื่อเราพิมพ์คำว่า Fu Manchu

Icelandie, Saratoga [ER] ติดกับท้ายไฟล์ .EXE โอกาสที่จะติดเชื้อจะประมาณ 1 ใน 10 (1 ใน 2 ในกรณี Saratoga) ไวรัสจะเช็คว่าฮาร์ดดิสค์มีขนาดเกิน 20 เมกะไบต์หรือไม่ ถ้าใช่จะมีการทำเครื่องหมาย Bad Cluster จำนวน 1 cluster ที่ FAT ชุดแรก

Italian, Pingpong, Turin, Bouncing Ball [DR]
จะใช้ดิสค์ที่บูตเซกเตอร์กับอีก 1 คลัสเตอร์ (2 เซกเตอร์) กับหน่วยความจำ 2K จะแสดงกระเด้งไปมา (Bouncing Ball) ตัวต้นแบบ (original version) ไม่สามารถทำงานบนเครื่อง 80286 และ 80386

Jerusalem, PLO, Friday the 13th, Israeli, sUMsDos [CER]
เพิ่มขนาดไฟล์ .COM ขึ้น 1813 ไบต์และ .EXE ขึ้น 1805 ไบต์ หลังจากทำงานไปประมาณ 30 นาที จะเกิดแบล็ควินโดว์ที่จุดเริ่มต้น 5,5 กับ 16,16 เครื่องจะช้าลงและเมื่อถึงวันศุกร์ที่ 13 โปรแกรมที่เรียกปฏิบัติงานจะถูกลบทิ้ง

Lehigh [CR] ติดกับ command.com เท่านั้นโดยเพิ่มขนาดขึ้น 555 ไบต์ ถ้าเกิดมีการติดเชื้อ 4 ครั้ง จะมีการทำลายข้อมูลของดิสค์ทั้งหมด (FAT และไดเรคทอรีถูกทำลาย)

Mistake [DR] ทำการเปลี่ยนข้อมูลเมื่อมีการสั่งพิมพ์ออกพรินเตอร์ (Virus awaiting disassembly)

MIX1 [ER] ติดกับไฟล์ .EXE เมื่อทำงานแล้วจะย้ายตัวเองไปไว้หน่วยความจำ [ถ้ามีโปรแกรมบางตัวใช้หน่วยความจำนี้ จะทำให้ระบบเสีย (crash) ไป] ไวรัสจะดักการทำงานของ interrupt service ที่เกี่ยวกับพรินเตอร์และการสื่อสารข้อมูลหลังจากทำงานไป 50 นาที คีย์ Num Lock และ Caps Lock จะถูกเซต หลังจากทำงานไป 60 นาทีจะเกิด Bouncing ball (คล้าย Italian) ท้ายไฟล์ที่ติดเชื้อจะมีข้อความ MIX1 ขนาดจะเปลี่ยนไปจาก 1618 จนถึง 1633 ไบต์

New Zealand, stoned, Marjuana [MR]
กินหน่วยความจำ 2K ติดที่ส่วนที่ทำการบูตระบบ (booting sector) เท่านั้น โดยบูตเซกเตอร์เดิมจะย้ายไปที่แทร็ก 0 เฮด 0 เซกเตอร์ 3 บนฟลอปปี้ดิสค์และแทร็ก 0 เฮด 0 เซกเตอร์ 2 บนฮาร์ดดิสค์ จะมีข้อความบนบูตเซกเตอร์ที่ติดเชื้อว่า Your PC is now Stoned ซึ่งข้อความนี้จะมีโอกาสขึ้นบนจอประมาณ 1 ใน 8 ครั้ง ในการบูตด้วยฟลอปปี้ดิสค์

Palette [CR] ติดไฟล์ .COM มีขนาดเพิ่มขึ้น 1538 ไบต์ (Virus awaiting disassembly)

Pentagon [DR] ใช้หน่วยความจำ 5 K อยู่ที่บูตเซกเตอร์กับอีก 2 ไฟล์ ติดเฉพาะดิสค์ 360 K จะเป็นตัวกำจัดไวรัส Brain (look for and remove Brain)

South African, Friday the 13th, Miami, Munich, Virus-B [CN]
ขนาดเพิ่มขึ้น 419 ไบต์ (แต่มีรายงานว่าขนาดจะอยู่ระหว่าง 415 ถึง 544 ไบต์) จะไม่ติดกับ command.com และไฟล์ที่เป็น read only

Spanish, 2930 - ยังไม่มีข้อมูล (Virus awaiting dessassembly)

Suriv 1.01, Israeli, April 1st COM [CR]
ติดเฉพาะไฟล์.COM ไม่ติด command.com มีขนาดเพิ่มขึ้น 897 ไบต์ ถ้าเกิดวันที่เป็น 1 เมษายน จะเกิดข้อความว่า "APRIL 1ST HA HA HA YOUR HAVE VIRUS" และเครื่องถูกจะหยุด (machine will lock) ถ้าเป็นหลังวันที่ 1 เมษายนจะขึ้นข้อความว่า "YOU HAVE A VIRUS!!!" แต่เครื่องจะไม่ถูกหยุด

Suriv 2.01, Israeli, April 1st EXE [ER]
ติดเฉพาะไฟล์ .EXE ขนาดเพิ่มขึ้น 1488 ไบต์ วันที่ 1 เมษา จะขึ้นข้อความว่า "APRIL 1ST HA HA HA YOU HAVE VIRUS" และถ้าปีเป็น 1980 (DOS default) หรือเป็นวันพุธหลังวันที่ 16 เมษายน 1988 เครื่องจะถูกหยุด เมื่อไวรัสทำงานไป 1 ชั่วโมง

Suriv 3.00, Israeli [CER] เป็นตัวแรกของ Jerusalem โดยติดกับ .COM (1813 ไบต์) และ .EXE (1808 ไบต์) แต่ผลการทำงานจะเกิดขึ้นภายใน 30 วินาทีแทนที่จะเป็น 30 นาที และไม่มีการลบโปรแกรมใด ๆ

Syslock [CEN] ติดกับไฟล์ .COM และ .EXE มีขนาดเพิ่มขึ้น 3551 ไบต์ โอกาสแพร่เชื้อประมาณ 1 ใน 4 ครั้งเมื่อไวรัสทำงาน ไวรัสมีการเข้ารหัสตัวเองไว้และจะไม่แพร่เชื้อเมื่อเราตั้งค่าสภาวะแวดล้อม (environment) ไว้เป็น SYSLOCK = @ →

รูปที่ 2 (ต่อ)

Trace Back [CER] ติดกับไฟล์ .COM และ .EXE มีขนาดเพิ่มขึ้น 3066 ไบต์และจะติดกับไฟล์ที่ถูกเรียกใช้งาน ในวันที่ 5 ธันวาคม หรือหลังจากนั้นไวรัสจะแพร่เชื้อกับไฟล์ .COM และ .EXE ในไดเรคทอรีปัจจุบัน (current directory) หรือไฟล์แรกที่เจอในไดเรคทอรีราก (root directory) วันที่ 28 ธันวาคม 1988 หรือหลังจากนั้นจะมีจอคล้าย cascade ไวรัส ถ้าเกิดเราไม่ได้พิมพ์ข้อมูลลงไป จอจะถูกเก็บไว้ภายใน 1 นาที และแสดงขึ้นมาอีกครั้งทุก 1 ชั่วโมง

Typo, Fumble [CR] ติดกับไฟล์ .COM ทุกไฟล์ทุกไดเรคทอรีย่อย (sub directory) ในวันที่ 1 ของทุกเดือน ขนาดเพิ่มขึ้น 867 ไบต์

Typoboot, Typo [B] ยังไม่มีข้อมูล

Vienna, Austrain, Unesco, DOS62, Lisbon [CN] มีขนาด 648 ไบต์ จะแพร่กับไฟล์ .COM ในไดเรคทอรีปัจจุบัน (current directory) และไดเรคทอรีที่เซตไว้ใน PATH

Yale, Alamda, Merrit [DR] กินหน่วยความจำ 1K ไม่สามารถทำงานบนเครื่อง 80286 และ 80386 บูตเซกเตอร์จริง (original boot sector) จะถูกย้ายไปที่แทร็ก 39 เฮด 0 เซกเตอร์ 8

Yankee [CER] ขนาดเพิ่มขึ้น 2885 ไบต์ ยังไม่มีข้อมูลเพิ่มเติม ไวรัสที่เหลือต่อไปนี้มีเฉพาะรายงาน (ไม่มีโปรแกรมที่ Virus Bulletin)

2730 [D]

4K, IDF, Israeli Defence Forces [CER] มีขนาด 4096 ไบต์

Century A เหมือนกับ Jerusalem C แต่จะทำงานเมื่อวันที่ 1 เดือนมกราคมปี 2000 และทำลาย FAT

Century B เหมือนกับ Century A แต่จะทำให้เกิดช่วงเวลาคอย (wait) เมื่อใช้โปรแกรม Backup.com

Disk Killer, Ogre จะขึ้นข้อความ "Disk Killer Version 1.00 by Ogre Software, April, 1989 Do not turn off the power or remove the diskette while processing"

Do-nothing [R]

Fallboot [D] อาการจะคล้ายกับ cascade รายงานโดยไอบีเอ็มด้วยโปรแกรม VIRSCAN

Ghostballs [CN] ขนาด 2351 ไบต์ บนตัวไวรัสจะมีข้อความว่า "GhostBalls, Product of Iceland"

Jerusalem A: ไม่แสดง black-hole

Jerusalem B: ไฟล์ .EXE จะถูกติดซ้ำได้ ข้อผิดพลาดในโปรแกรม (Bugs) ถูกแก้ไข

Jerusalem C: ไม่ทำให้เครื่องช้าลง

Jerusalem D: ทำลาย FAT

Jerusalem E: ทำลาย FAT ในปี 1990

MachoSoft [CEN] เปลี่ยนคำว่า MicroSoft เป็น MachoSoft ทุกครั้งที่เจอบนฮาร์ดดิสก์ จะค้นหาทีละ 20 เซกเตอร์และเก็บเซกเตอร์สุดท้ายที่ค้นหาไปแล้วไว้บนไฟล์ IBMNETIO.SYS ซึ่งถูกเซตเป็น hidden และ system ไฟล์ ถ้าไวรัสค้นหาถึงเซกเตอร์สุดท้ายก็จะเริ่มเซกเตอร์แรกใหม่ เหตุการณ์นี้จะเกิดขึ้นหลัง 1 มกราคม 1985 และตัวแปรสิ่งแวดล้อม (environment variable) ชื่อ VIRUS ไม่ได้ถูกเซตเป็น OFF ไวรัสจะมีขนาด 3550 ถึง 3560 ไบต์

Missouni [D]

Nichols [D]

Oropax, Music Virus [CR] มีขนาด 2756 ถึง 2806 ความยาวของไฟล์ทั้งหมดจะสามารถหารด้วย 51 ลงตัว หลังจากไวรัสทำงาน 5 นาที จะเกิดเสียง 3 แบบในทุก ๆ 7 นาที

Screen [CR] ติดกับไฟล์ .COM สลับตัวเลข 2 ตัวบนจอภาพ

Sunday [CER] มีขนาด 1631 (บางรายงานบอกว่า 1644) จะทำงานในวันอาทิตย์ขึ้นข้อความว่า "Today is Sunday! Why do you work so hard? All work and no play make you a dull boy"

SWAP [DR] กินหน่วยความจำ 2K จะ Bad cluster ที่แทร็ก 39, เซกเตอร์ 6 และ 7 (ไม่ระบุ head) จะแพร่เชื้อหลังจากบูตระบบไปแล้ว 10 นาที

Vacsina [CER] ไฟล์ .COM จะมีขนาดเพิ่มขึ้น 1206 ถึง 1221 และไฟล์ .EXE จะมีขนาดเพิ่มขึ้น 1338 ถึง 1353 ไบต์ หลังจากแพร่เชื้อใส่ไฟล์ .COM สำเร็จจะเกิดเสียงดังขึ้น (bell is sounded) จะติดไฟล์ที่ถูกเรียกปฏิบัติงานผ่าน INT 21 ฟังก์ชัน 4B (load and execute) เช่น COM, EXE, OVL และ APP (GEM) ก่อนจะแพร่เชื้อจะเช็คว่าไฟล์นั้นติดเชื้อในรุ่นก่อนหรือไม่ ถ้าติดอยู่แล้วจะเปลี่ยนเป็นรุ่นใหม่แทน (ปัจจุบันเป็นรุ่น 5)